

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
Information associated with)
elbozz14@icloud.com, as further described in)
Attachment A)

Case No. **24-M-317 (SCD)****WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 2-20-24 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____

Hon. Stephen C. Dries
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 2-6-24. 10:50 am

Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with elbozz14@icloud.com (“**TARGET ACCOUNT**”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. (“Apple”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the accounts were created, the length of service, the IP address used to register the accounts, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the accounts (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);
- c. The contents of all emails associated with the accounts from January 1, 2023 to the present, including stored or preserved copies of emails sent to and from the accounts (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;
- d. The contents of all instant messages associated with the accounts from January 1, 2023 to the present, including stored or preserved copies of instant messages

(including iMessages, SMS messages, and MMS messages) sent to and from the accounts (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

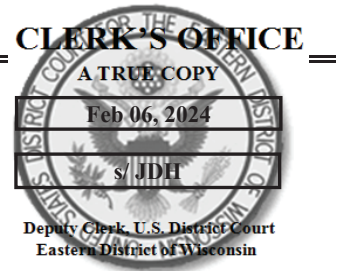
- e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- f. All activity, connection, and transactional logs for the accounts (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;
- g. All records and information regarding locations where the accounts or devices associated with the accounts were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
- h. All records pertaining to the types of service used;
- i. All records pertaining to communications between Apple and any person regarding the accounts, including contacts with support services and records of actions taken; and
- j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 21, United States Code, Sections 841(a)(1), 843(b) and 846, those violations involving Damian DEL VALLE-RIVERA and others known and unknown, and occurring after January 1, 2023, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) The sale of illegal drugs and the laundering of proceeds of drug sales;
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the user ID about matters relating to drug trafficking, including records that help reveal their whereabouts.



UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. **24-M-317 (SCD)**

Information associated with elbozz14@icloud.com,
as further described in Attachment A

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 U.S.C. §§ 841(a)(1); 846; & 843(b)	Possession with the intent to distribute controlled substances; Conspiracy to possess with the intent to distribute controlled substances; and Unlawful use of a communication facility in furtherance of drug trafficking.

The application is based on these facts:

See Attachment A.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Tyler Fink

Digitally signed by Tyler Fink
Date: 2024.02.05 11:44:25 -06'00'

Applicant's signature

Tyler Fink, USPIS Insp.

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 2-6-24

Stephen C. Dries

Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Tyler Fink, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. (“Apple”), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Postal Inspector with the United States Postal Inspection Service (“USPIS”). I have been employed as a full-time law enforcement officer since June 2014.

3. The USPIS is the primary investigative arm of the United States Postal Service (“USPS”) and is charged under Title 18, United States Code, 3061 with the enforcement of laws governing the use and movement of the United States Mail, including, but not limited to, the misuse and fraudulent schemes involving the mail, crimes relating to mail fraud, identity theft, and narcotics trafficking involving the U.S. Mail.

4. I am currently assigned to the USPIS Milwaukee Office, Multi-function team, as well as being placed on the High Intensity Drug Trafficking Area (“HIDTA”) Interdiction Task Force. The USPIS Milwaukee Office investigates USPS customers involving narcotics, prohibited mailings, controlled substances, and other matters related to the Postal Service. The Milwaukee office’s team has intercepted numerous parcels, which were found to contain narcotics or proceeds of narcotics trafficking and other criminal activity.

5. I have participated in numerous complex narcotics investigations which involved violations of state and federal controlled substances laws including Title 21, United States Code, Sections 841(a)(1) and 846 (possession with intent to distribute a controlled substance and conspiracy to possess with intent to distribute a controlled substance), and other related offenses. I have had both formal training and have participated in numerous complex drug trafficking investigations, including ones using wiretaps.

6. As a part of my duties, I investigate criminal violations relating to narcotics trafficking offenses, including violations of Title 21, United States Code, Sections 841, 843, and 846, and federal firearms offenses, including violations of Title 18, United States Code, Sections 922(g), 924(a), and 924(c). In the course of my experience, I have and continue to be involved in investigations of criminal offenses and have assisted with search warrants for items related to gang investigations, organized crime, violent crime, firearms offenses, drug trafficking, including cellular telephones and other electronic telecommunication devices.

7. I have had formal training in the investigation of drug trafficking. I have worked with informants in the investigation of drug trafficking. I have participated in the execution of numerous search warrants in which controlled substances, firearms, drug paraphernalia, and monies were seized.

8. This affidavit is based upon my personal knowledge and upon information provided to me by other federal, state, and local law enforcement officers during the course of their official duties. Throughout this affidavit, I refer to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom I have had regular contact regarding this investigation.

9. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

10. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Section 841(a)(1), 843(b), and 846 have been committed by Damian DEL VALLE-RIVERA (“DEL VALLE-RIVERA”) and others known and unknown. There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

11. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

12. Case agents are currently investigating Joseph DEL VALLE-MARTINEZ (DOB: 06/02/1997), who is receiving cocaine in the Eastern District of Wisconsin.

13. In November 2023, case agents initiated an investigation into Damian DEL VALLE-RIVERA (DOB: 09/22/2000), who was identified by case agents as a person who was shipping large amounts of cocaine to Milwaukee, Wisconsin and Bakersfield, California.

Suspicious Parcels – SUBJECT PARCEL 1 and SUBJECT PARCEL 2

14. On November 27, 2023, I was reviewing U.S. Postal Service (“USPS”) business records when the following two parcels were found to be suspicious:

- a. USPS Priority Mail parcel 9505516209493328222953 (“SUBJECT PARCEL 1”).
SUBJECT PARCEL 1 was a USPS large flat rate parcel weighing approximately 7 lbs. 10 oz. The shipping label for SUBJECT PARCEL 1 indicated it was from “Jose Ortiz 19 Calle Ramon Rivera Cruz Urb. San Pedro Toa Baja, PR 00949”. SUBJECT PARCEL 1 bore a handwritten label addressed to “Maria Ortiz 3210A S 12th St Milwaukee WI 53215-4608”. SUBJECT PARCEL 1 was postmarked on November 24, 2023, in San Juan, Puerto Rico 00936 at approximately 10:31 a.m. The postage paid was \$22.80. SUBJECT PARCEL 1 was delivered on November 28, 2023, at approximately 12:04 PM.
- b. USPS Priority Mail parcel 9505512222093328912521 (“SUBJECT PARCEL 2”).
SUBJECT PARCEL 2 was a USPS large flat rate parcel weighing approximately 7 lbs. 3 oz. The shipping label for SUBJECT PARCEL 2 indicated it was from “Jose Ortiz 19 Calle Ramon Rivera Cruz Urb. San Pedro Toa Baja, PR 00949”. SUBJECT PARCEL 2 bore a handwritten label addressed to “Maria Ortiz 3210A S 12th St Milwaukee WI 53215-4608”. SUBJECT PARCEL 2 was postmarked on November 24, 2023, in Bayamon, Puerto Rico 00959 at approximately 11:39 a.m. The postage paid was \$22.80.

15. The Consolidated Lead Evaluation and Reporting (“CLEAR”) database is a public records product which is designed for law enforcement officers in locating subjects and witnesses, verifying identities of individuals, and gathering background information for use in investigations. A search of the CLEAR database revealed the sender and recipient names shown on the shipping labels for SUBJECT PARCEL 1 and SUBJECT PARCEL 2 were fictitious.

16. Using an internet search engine, it showed the San Juan Post Office, located at 585 Avenue RD Roosevelt, San Juan, Puerto Rico 00936, which is the postmark location for SUBJECT PARCEL 1, is approximately a 15-minute drive from the Bayamon Post Office, located at 100 Avenue Ramon L. Rodriguez, Bayamon, Puerto Rico 00959, which is the postmark location for SUBJECT PARCEL 2. SUBJECT PARCEL 1 was postmarked approximately 68 minutes before SUBJECT PARCEL 2. From my training and experience, I believe the subject(s) shipping SUBJECT PARCEL 1 and SUBJECT PARCEL 2 intentionally visited two different nearby post offices in order to conceal their participation, and the contents of the parcels.

17. On November 29, 2023, case agents conducted surveillance on the delivery of SUBJECT PARCEL 2. At approximately 12:22 p.m., case agents observed the USPS letter carrier deliver SUBJECT PARCEL 2 by placing it directly in front of the entrance door on the south side of 3210A S 12th Street. At approximately 12:54 p.m., case agents observed a Hispanic female exit this door, pick up SUBJECT PARCEL 2, and bring it into the residence.

18. A review of historical USPS parcels delivered to 3210A S 12th Street indicated previous parcels were addressed to a Patricia Nolasco. The Wisconsin Department of Transportation records indicated a Patricia G. NOLASCO-BRITO has her address on record as 3210A S 12th Street, Milwaukee, Wisconsin. Case agents compared NOLASCO-BRITO’s

Wisconsin driver license photograph to the female who took possession of SUBJECT PARCEL 2. Case agents identified NOLASCO-BRITO as this female.

19. On December 7, 2023, I received a copy of the surveillance video from the USPS San Juan, Puerto Rico Post Office showing SUBJECT PARCEL 1 being shipped. I reviewed the video which showed Damian DEL VALLE-RIVERA shipping SUBJECT PARCEL 1. DEL VALLE-RIVERA was driving a white 2019 Acura MDX SUV with tinted windows bearing Puerto Rico license plate JJO514. A review of the Puerto Rico vehicle registration records indicated the vehicle is registered to DEL VALLE-RIVERA. I was able to later identify DEL VALLE-RIVERA from his Puerto Rico driver's license photograph.

20. On this same date, I also received a copy of the surveillance video from the USPS Bayamon, Puerto Rico Post Office showing SUBJECT PARCEL 2 being shipped. I reviewed the video which also showed DEL VALLE-RIVERA ship SUBJECT PARCEL 2. DEL VALLE-RIVERA was again appearing to be driving his white 2019 Acura MDX SUV with tinted windows.

Cocaine Seizure and Suspicious Parcel – SUBJECT PARCEL 3 and SUBJECT PARCEL 4

21. On November 30, 2023, I was reviewing the USPS business records when the following parcel was found to be suspicious: USPS Priority Mail parcel 9505511455113331418724 ("SUBJECT PARCEL 3"). SUBJECT PARCEL 3 was a USPS large flat rate parcel weighing approximately 6 lbs. 15 oz. The shipping label for SUBJECT PARCEL 3 indicated it was from "Jose Ortiz 20 Calle Ramon Rivera Cruz Urb. San Pedro Toa Baja, PR 00949". SUBJECT PARCEL 3 bore a handwritten label addressed to "Maria Ortiz 3210A S 12th St. Milwaukee WI 53215-4608". SUBJECT PARCEL 3 was postmarked on November 27, 2023, in Toa Alta, Puerto Rico 00953 at approximately 9:14 a.m. The postage paid was \$22.80.

22. A search of the CLEAR database revealed the sender and recipient names shown on the shipping label for SUBJECT PARCEL 3 were fictitious.

23. On November 30, 2023, case agents conducted surveillance on the delivery of SUBJECT PARCEL 3. At approximately 11:40 a.m., the USPS letter carrier delivered SUBJECT PARCEL 3 by placing it directly in front of the entrance door on the south side of 3210A S 12th Street. At approximately 12:15 p.m., I observed NOLASCO-BRITO exit this door, pick up SUBJECT PARCEL 3, and bring it into the residence.

24. USPS business records which indicated the customer who shipped SUBJECT PARCEL 3 also shipped the following suspicious parcel at the same time under the same transaction: USPS Priority Mail parcel 9505511455113331418700 (“SUBJECT PARCEL 4”). SUBJECT PARCEL 4 was a USPS large flat rate parcel weighing approximately 5 lbs. 0 oz. The shipping label for SUBJECT PARCEL 4 indicated it was from “Jose Ortiz 20 Calle Ramon Rivera Cruz Urb. San Pedro Toa Baja, PR 00949”. SUBJECT PARCEL 4 bore a handwritten label addressed to “Maria Ortiz 1705 Crestview Dr Bakersfield, CA 93305”. SUBJECT PARCEL 4 was postmarked on November 27, 2023, in Toa Alta, Puerto Rico 00953 at approximately 9:14 a.m. The postage paid was \$22.80.

25. A search of the CLEAR database revealed the sender and recipient names shown on the shipping label for SUBJECT PARCEL 4 were fictitious.

26. On November 30, 2023, I contacted Bakersfield, California Postal Inspector Louie Martinez and requested he inspect SUBJECT PARCEL 4 for further scrutiny. On this same date, Inspector Martinez located SUBJECT PARCEL 4 in Bakersfield and agreed it was suspicious in nature. Inspector Martinez applied for and received a federal search warrant for SUBJECT

PARCEL 4. The search warrant was issued by U.S. Magistrate Judge Christopher Baker in the Eastern District of California.

27. Upon executing the search warrant on SUBJECT PARCEL 4, case agents discovered one vacuum sealed bag of a white powdery substance, suspected to be cocaine. The suspected cocaine was still in a brick like form. The brick of suspected cocaine had a gross weight of approximately 1,039 grams. The suspected cocaine was field tested using a Thermo Scientific TruNarc Analyzer and presumptively field tested positive for cocaine HCl.

28. On December 7, 2023, I received a copy of the surveillance video from the USPS Toa Alta, Puerto Rico Post Office showing SUBJECT PARCEL 3 and SUBJECT PARCEL 4 being shipped. I reviewed the video which showed DEL VALLE-RIVERA shipping both parcels. DEL VALLE-RIVERA appeared to be driving his white 2019 Acura MDX SUV with tinted windows.

Suspicious Parcels – SUBJECT PARCEL 5, SUBJECT PARCEL 6, and SUBJECT PARCEL 7

29. On December 6, 2023, I was reviewing the USPS business records when the following three parcels below were found to be suspicious:

- a. USPS Priority Mail Express parcel EI526990005US (“SUBJECT PARCEL 5”). SUBJECT PARCEL 5 was a USPS large flat rate parcel weighing approximately 8 lbs. 4 oz. The shipping label for SUBJECT PARCEL 5 indicated it was from “Maria Ortiz 18 Calle Ramon Rivera Cruz Urb San Pedro Toa Baja, PR 00949”. SUBJECT PARCEL 5 bore a handwritten label addressed to “Damian Del Valle 1033 S 76th St Milwaukee, WI 53214”. SUBJECT PARCEL 5 was postmarked on December 5, 2023, in Dorado, Puerto Rico 00646 at approximately 9:37 a.m. The

postage paid was \$115.05. SUBJECT PARCEL 5 was delivered on December 6, 2023, at approximately 12:29 p.m.

- b. USPS Priority Mail Express parcel EI526985014US (“SUBJECT PARCEL 6”). SUBJECT PARCEL 6 was a USPS large flat rate parcel weighing approximately 7 lbs. 13 oz. The shipping label for SUBJECT PARCEL 6 indicated it was from “Maria Ortiz 18 Calle Ramon Rivera Cruz Urb San Pedro Toa Baja, PR 00949”. SUBJECT PARCEL 6 bore a handwritten label addressed to “Damian Del Valle 1033 S 76th St Milwaukee, WI 53214”. SUBJECT PARCEL 6 was postmarked on December 5, 2023, in Sabana Seca, Puerto Rico 00952 at approximately 10:03 a.m. The postage paid was \$107.15. SUBJECT PARCEL 6 was delivered on December 6, 2023, at approximately 12:29 p.m.

- c. USPS Priority Mail Express parcel EI526985031US (“SUBJECT PARCEL 7”). SUBJECT PARCEL 7 was a USPS large flat rate parcel weighing approximately 6 lbs. 15 oz. The shipping label for SUBJECT PARCEL 7 indicated it was from “Damian Del Valle 18 Calle Ramon Rivera Cruz Urb. San Pedro Toa Baja, P.R 00949”. SUBJECT PARCEL 7 bore a handwritten label addressed to “Joseph Del Valle 3210 S 12th St. Milwaukee, WI 53215-4608”. SUBJECT PARCEL 7 was postmarked on December 5, 2023, in Sabana Seca, Puerto Rico 00952 at approximately 11:03 a.m. The postage paid was \$99.30. SUBJECT PARCEL 7 was delivered on December 6, 2023, at approximately 2:32 p.m.

30. A search of the CLEAR database revealed the sender and recipient names shown on the shipping labels for SUBJECT PARCEL 5, SUBJECT PARCEL 6, and SUBJECT PARCEL 7 were all fictitious except for the recipient’s name for SUBJECT PARCEL 7. The Wisconsin

Department of Transportation records showed a Joseph DEL VALLE-MARTINEZ (“DEL VALLE-MARTINEZ”) has his address on record as 3210A S 12th Street, Milwaukee, Wisconsin 53215.

31. Using an internet search engine, it showed the Dorado Post Office, located at 100 CARR 698, Dorado, Puerto Rico 00646, which is the postmark location for SUBJECT PARCEL 5, is approximately an 18-minute drive from the Sabana Seca Post Office, located at 100 CARR 866, Sabana Seca, Puerto Rico 00952, which is the postmark location for SUBJECT PARCEL 6 and SUBJECT PARCEL 7. SUBJECT PARCEL 5 was postmarked approximately 26 minutes before SUBJECT PARCEL 6. From my training and experience, I believe the subjects shipping the above-mentioned parcels intentionally visited two different nearby post offices in order to conceal their participation, and the contents of the parcels.

32. On December 28, 2023, I received a copy of the surveillance video from the USPS Dorado, Puerto Rico Post Office showing SUBJECT PARCEL 5 being shipped. I reviewed the video which showed an unknown female exit the front passenger seat of a white 2019 Acura MDX SUV with tinted windows bearing Puerto Rico license plate JJO514 registered to DEL VALLE-RIVERA. The female entered the Post Office and shipped SUBJECT PARCEL 5.

33. On December 28, 2023, I received a copy of the surveillance video from the USPS Sabana Seca, Puerto Rico Post Office showing SUBJECT PARCEL 6 and SUBJECT PARCEL 7 being shipped. I reviewed the video which showed an unknown female exit the front passenger seat of a white 2019 Acura MDX SUV with tinted windows bearing Puerto Rico license plate JJO514 registered to DEL VALLE-RIVERA. The female entered the Post Office and shipped SUBJECT PARCEL 6. This is the same female that previously shipped SUBJECT PARCEL 5 on the same date at a different Post Office location. The video for SUBJECT PARCEL 7 showed

DEL VALLE-RIVERA arriving in the same white Acura MDX, enter the Post Office, and ship SUBJECT PARCEL 7.

Two Cocaine Seizures – SUBJECT PARCEL 8 and SUBJECT PARCEL 9

34. On January 11, 2024, I was reviewing the USPS business records when the following two parcels below were found to be suspicious.

- a. USPS Priority Mail parcel 9505511455824010538953 (“SUBJECT PARCEL 8”).

SUBJECT PARCEL 8 was a USPS large flat rate parcel weighing approximately 6 lbs. 2 oz. The shipping label for SUBJECT PARCEL 8 indicated it was from “Vanessa Ortiz 20 Calle Ramon Rivera Cruz Urb. San Pedro Toa Baja, P.R. 00949”. SUBJECT PARCEL 8 bore a handwritten label addressed to “Maria Ortiz 3210A S 12th St, Milwaukee, WI 53215-4608”. SUBJECT PARCEL 8 was postmarked on January 10, 2024, in Toa Baja, Puerto Rico 00949 at approximately 11:36 a.m. The postage paid was \$22.80.

- b. USPS Priority Mail Express parcel EI526988041US (“SUBJECT PARCEL 9”).

SUBJECT PARCEL 9 was a USPS parcel weighing approximately 7 lbs. 9 oz. The shipping label for SUBJECT PARCEL 9 indicated it was from “Kevin Ortiz 19 Calle Ramon Rivera Cruz Urb. San Pedro Toa Baja, P.R. 00949”. SUBJECT PARCEL 9 bore a handwritten label addressed to “Maria Ortiz 3210A S 12th St, Milwaukee, WI 53215-4608”. SUBJECT PARCEL 9 was postmarked on January 11, 2024, in Dorado, Puerto Rico 00646 at approximately 11:47 a.m. The postage paid was \$107.15.

35. A search of the CLEAR database revealed the sender and recipient names shown on the shipping labels for SUBJECT PARCEL 8 and SUBJECT PARCEL 9 were fictitious.

36. On Saturday, January 13, 2024, I traveled to the Milwaukee Processing and Distribution Center, located at 345 W. Saint Paul Avenue, Milwaukee, Wisconsin 53203, and located SUBJECT PARCEL 9.

37. On January 16, 2024, case agents applied for and received a federal search warrant for SUBJECT PARCEL 9. The search warrant was issued by United States Magistrate Judge William Duffin in the Eastern District of Wisconsin.

38. Upon executing the search warrant on SUBJECT PARCEL 9, on January 16, 2024, case agents discovered one vacuum sealed bag of a white powdery substance, suspected to be cocaine, wrapped in multiple layers of vacuum sealed bags and carbon paper. The suspected cocaine was secreted inside of a set of bed sheets within SUBJECT PARCEL 9. The suspected cocaine was still in a brick like form. The “kilo” stamp on one side appeared to be “48 SUTAN” and the other side had a crosshatch pattern stamped into it. The brick of suspected cocaine had a gross weight of approximately 1,020 grams. The suspected cocaine was field tested by case agents using a field test pouch kit (Nark #07) and field tested positive for cocaine.

39. I repackaged SUBJECT PARCEL 9 with sham in preparation of a controlled delivery.

40. A review of USPS business records indicated on January 13, 2024, an unknown subject(s) contacted USPS and inquired on the delivery status of SUBJECT PARCEL 9. The subject(s) requested updates be sent to email address elbozz14@icloud.com (**TARGET ACCOUNT**).

41. A search of a law enforcement database indicated the **TARGET ACCOUNT** is listed to a Damian DEL VALLE.

42. On January 22, 2024, I received a copy of the surveillance video from the USPS Dorado, Puerto Rico Post Office showing SUBJECT PARCEL 9 being shipped. I reviewed the video which showed DEL VALLE-RIVERA shipped SUBJECT PARCEL 9.

43. On January 17, 2024, I traveled to the West Milwaukee Post Office, located at 4300 W. Lincoln Avenue, Milwaukee, Wisconsin 53219, and located SUBJECT PARCEL 8.

44. On January 17, 2024, I applied for a federal search warrant for SUBJECT PARCEL 8. On January 19, 2024, the search warrant was issued by United States Magistrate Judge William Duffin in the Eastern District of Wisconsin.

45. Upon executing the search warrant on SUBJECT PARCEL 8, on January 19, 2024, case agents discovered one vacuum sealed bag of a white powdery substance, suspected to be cocaine, wrapped in multiple layers of vacuum sealed bags, what appeared to be a shiny mylar bag, tape, and carbon paper. The suspected cocaine was secreted inside of a set of bed sheets within SUBJECT PARCEL 8. The suspected cocaine was still in a brick like form. The “kilo” stamp appeared to be “100%” over “★★★★★”. The brick of suspected cocaine had a gross weight of approximately 1,020 grams. The suspected cocaine was field tested by case agents using a field test pouch kit (Nark #07) and field tested positive for the presence of cocaine.

46. Due to SUBJECT PARCEL 8 not arriving in Milwaukee until January 17, 2024, this parcel was not delivered during the controlled delivery below.

47. On January 22, 2024, I received a copy of the surveillance video from the USPS Toa Baja, Puerto Rico Post Office showing SUBJECT PARCEL 8 being shipped. I reviewed the video which showed an unknown female shipped SUBJECT PARCEL 8.

Controlled Delivery and Residential Search Warrant

48. On January 16, 2024, I applied for and received a search warrant for 3210A S. 12th Street, Milwaukee, Wisconsin 53215. The search warrant was issued by Honorable Barry Phillips, Judicial Court Commissioner of the Judicial District of Wisconsin.

49. On January 17, 2024, while acting in an undercover capacity, Postal Inspector Chris Massari dressed as a USPS Letter Carrier and drove a USPS delivery vehicle to conduct a controlled delivery with SUBJECT PARCEL 9. At approximately 10:45 a.m., Inspector Massari knocked on the door and rang the doorbell of 3210A S 12th Street. There was no initial answer, therefore Inspector Massari delivered the parcel by placing it in front of the door. Inspector Massari then left the area while other case agents continued surveillance.

50. At approximately 11:15 a.m., case agents observed Patricia NOLASCO-BRITO stick her head out of a window from the second floor and appear to look in the area of where SUBJECT PARCEL 9 was delivered. Case agents then observed NOLASCO-BRITO exit the south facing door of 3210A S 12th Street, pick up SUBJECT PARCEL 9, and bring the parcel into the residence.

51. At approximately 11:20 a.m., law enforcement officers executed the search warrant at this location. The entry team cleared the residence and located NOLASCO-BRITO, her two juvenile children, and SUBJECT PARCEL 9 inside.

Mirandized Interview of Patricia NOLASCO-BRITO

52. On January 17, 2024, NOLASCO-BRITO was interviewed by case agents while investigators were conducting a search at her residence. Case agents read NOLASCO-BRITO her *Miranda* rights. After being read her rights, NOLASCO-BRITO stated she understood her rights and was willing to speak with the case agents. NOLASCO-BRITO stated on the date of the search warrant she was at home with her two children, and she was Face Timing her fiancé DEL VALLE-

MARTINEZ. She was told by DEL VALLE-MARTINEZ that a package was delivered to their residence and he requested she go get it because it was for his cousin. NOLASCO-BRITO then walked outside, grabbed the package, brought the package into her home, and sent pictures of the box to DEL VALLE-MARTINEZ at his request. NOLASCO-BRITO estimated she has accepted five other packages just like the one she accepted before the search warrant and sent photographs of the packages to DEL VALLE-MARTINEZ each time. NOLASCO-BRITO said each time a package comes addressed to a person not living at the house she assumes they are for DEL VALLE-MARTINEZ's cousin.

Mirandized Interview of Joseph DEL VALLE-MARTINEZ

53. On January 17, 2024, Joseph DEL VALLE-MARTINEZ was voluntarily interviewed by investigators while not in custody. Case agents read DEL VALLE-MARTINEZ his *Miranda* rights. After being read his rights, DEL VALLE-MARTINEZ stated he understood his rights and was willing to speak. DEL VALLE-MARTINEZ said he was expecting one USPS parcel to be delivered to his residence. He explained his cousin, DEL VALLE-RIVERA, called him one day prior and told him he shipped him the package. DEL VALLE-MARTINEZ stated he knew the package contained illegal drugs, but he claimed he did not know what kind of drug or what quantity. DEL VALLE-MARTINEZ stated DEL VALLE-RIVERA has shipped him approximately six or seven USPS packages that he believed all contained some sort of illegal drugs. DEL VALLE-MARTINEZ said all of the packages came from Puerto Rico and all had fictitious names on them. He claimed he never orders the drugs from DEL VALLE-RIVERA, but DEL VALLE-RIVERA will ship the USPS packages and call DEL VALLE-MARTINEZ to let him know they are on the way. He explained DEL VALLE-RIVERA always tracks the packages and tells him when they get delivered to his home. DEL VALLE-MARTINEZ stated out of all of

the packages shipped to him by DEL VALLE-RIVERA, he only partially opened one of them and saw it contained bed sheets. He said he did not continue looking to see what else the package contained or if there was anything in the bed sheets. After the package gets shipped and DEL VALLE-RIVERA calls him, DEL VALLE-MARTINEZ stated his fiancé, NOLASCO-BRITO, will accept the package upon delivery and leave it at their house. DEL VALLE-MARTINEZ will notify DEL VALLE-RIVERA he has the package, and DEL VALLE-RIVERA will then fly from Puerto Rico to Chicago or Milwaukee and come to his house. DEL VALLE-MARTINEZ said once DEL VALLE-RIVERA gets to his house he will take possession of the USPS package and later drive it to Omaha, Nebraska. DEL VALLE-MARTINEZ further stated he believed DEL VALLE-RIVERA was currently in Milwaukee due to the package being delivered to his house today. He said he did not know where DEL VALLE-RIVERA was staying, but he usually stays at an unknown hotel. DEL VALLE-MARTINEZ added he believes DEL VALLE-RIVERA flies to an unknown city in California to also take possession of USPS packages he ships there with drugs.

USPS Parcels Related to Cocaine Seizure

54. On January 22, 2024, I reviewed USPS business records which indicated the following additional USPS parcel was linked to SUBJECT PARCEL 8 and SUBJECT PARCEL 9: USPS Priority Mail parcel 9405536105536070296217 (“SUBJECT PARCEL 11”). SUBJECT PARCEL 11 was a USPS parcel weighing approximately 4 lbs. 9 oz. The shipping label for SUBJECT PARCEL 11 indicated it was from “VICTOR MEDRANO 24813 APPLE ST SANTA CLARITA CA 91321”. SUBJECT PARCEL 11 bore a typewritten label addressed to “DAMIAN DEL VALLE PO Box 524, TOA BAJA PR 00951”. SUBJECT PARCEL 11 was postmarked on January 4, 2024, in Santa Clarita, California 91383 at approximately 4:22 p.m. The postage paid

was \$31.09. SUBJECT PARCEL 11 was delivered on January 9, 2024 at approximately 12:10 p.m.

55. The USPS PO Box registration records showed this box is currently registered to a customer named Francisco Felix Negrón with an email address of ELBO2214@icloud.com. It is unknown if the PO Box registration paperwork was handwritten by the customer and filled out as ELBO2214@icloud.com or ELBOZZ14@icloud.com (**TARGET ACCOUNT**). Due to the similarity of “2” and “Z”, it may have been improperly transferred from the PO Box registration form into the electronic USPS database. A copy of the registration form was not available for review.

56. Due to SUBJECT PARCEL 11 being addressed to a Damian DEL VALLE at a PO Box with an email address similar to **TARGET ACCOUNT**, DEL VALLE-RIVERA shipping a parcel containing approximately one “kilo” of suspected cocaine which was monitored by **TARGET ACCOUNT**, and a law enforcement database showing DEL VALLE-RIVERA is associated with **TARGET ACCOUNT**, I believe **TARGET ACCOUNT** is associated with DEL VALLE-RIVERA.

57. A review of USPS business records indicated 3210A S 12th Street has received several suspicious USPS parcels since February 2023. These previous parcels have multiple similar characteristics as the parcels previously seized by case agents in this investigation. These additional parcels were all shipped from the same vicinity in Puerto Rico, were approximately the same size, were shipped using the same mail class, and all of them were paid for in cash. Due to these factors, case agents believe all of these previous suspicious parcels contained cocaine.

BACKGROUND CONCERNING APPLE¹

58. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

59. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.
- c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create,

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

- d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.
- e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.
- f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.
- g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

60. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

61. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

62. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

63. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of

other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

64. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user’s photos and videos, iMessages, Short Message Service (“SMS”) and Multimedia Messaging Service (“MMS”) messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user’s instant messages on iCloud Drive. Some of this data is stored on Apple’s servers in an encrypted form but can nonetheless be decrypted by Apple.

65. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the

files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

66. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

67. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

68. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan

to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

69. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

70. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

71. Based on the forgoing, I request that the Court issue the proposed search warrant.

72. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with elbozz14@icloud.com (“**TARGET ACCOUNT**”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. (“Apple”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the accounts were created, the length of service, the IP address used to register the accounts, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the accounts (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);
- c. The contents of all emails associated with the accounts from January 1, 2023 to the present, including stored or preserved copies of emails sent to and from the accounts (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

- d. The contents of all instant messages associated with the accounts from January 1, 2023 to the present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the accounts (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;
- e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- f. All activity, connection, and transactional logs for the accounts (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;
- g. All records and information regarding locations where the accounts or devices associated with the accounts were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
- h. All records pertaining to the types of service used;
- i. All records pertaining to communications between Apple and any person regarding the accounts, including contacts with support services and records of actions taken; and
- j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 21, United States Code, Sections 841(a)(1), 843(b) and 846, those violations involving Damian DEL VALLE-RIVERA and others known and unknown, and occurring after January 1, 2023, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) The sale of illegal drugs and the laundering of proceeds of drug sales;
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the user ID about matters relating to drug trafficking, including records that help reveal their whereabouts.